(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 September 2003 (18.09.2003)

PCT

(10) International Publication Number
WO 03/077470 A1

(51) International Patent Classification[7]: H04L 9/08

(21) International Application Number: PCT/IB03/00655

(22) International Filing Date: 14 February 2003 (14.02.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
02075983.3 13 March 2002 (13.03.2002) EP

(71) Applicant *(for all designated States except US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **TUYLS, Pim, T.** [BE/NL]; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **KEVENAAR, Thomas, A., M.** [NL/NL]; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **SCHRIJEN, Geert, J.** [NL/NL]; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **VAN DIJK, Marten, E.** [NL/NL]; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: **GROENENDAAL, Antonius, W., M.**; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

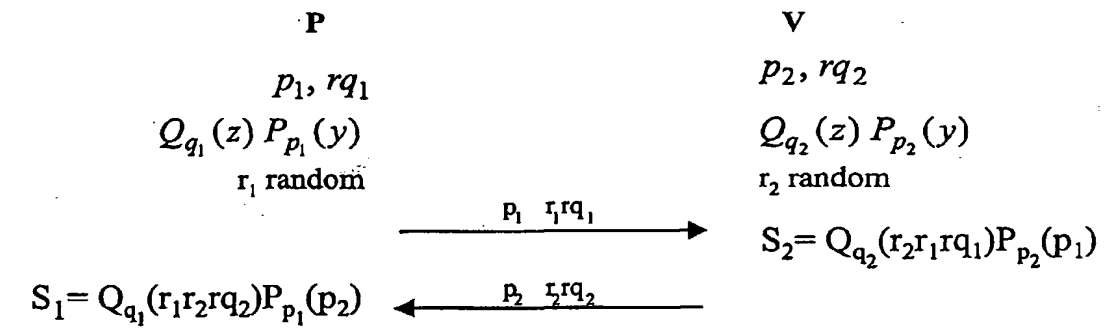
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: POLYNOMIAL-BASED MULTI-USER KEY GENERATION AND AUTHENTICATION METHOD AND SYSTEM



(57) Abstract: A method of generating a common secret between a first party and a second party, preferably devices (101-105) in a home network (100) that operate in accordance with a Digital Rights Management (DRM) framework. The devices calculate the common secret by evaluating the product of two polynomials P(x, y) and Q(x, z) using parameters previously distributed by a Trusted Third Party (TTP) and parameters obtained from the other party. Preferably the parties subsequently verify that the other party has generated the same secret using a zero-knowledge protocol or a commitment-based protocol. The method is particularly suitable for very low power devices such as Chip-In-Disc type devices.

WO 03/077470 A1